

1 **The Claims**

2  
3 1-2. (Canceled)

4  
5 3. (Previously presented) A computerized method for key-based  
6 secure storage comprising:

7 downloading information and an access predicate that specifies  
8 requirements for an application to access the information;

9 generating a seed value;

10 producing a hash seed value based on the seed value using a one-way hash  
11 function;

12 generating an application storage key from the hash seed value;

13 encrypting the information using the application storage key; and

14 associating the access predicate with the encrypted information.  
15

16 4. (Previously presented) A computerized method for key-based  
17 secure storage comprising:

18 downloading information and an access predicate that specifies  
19 requirements for an application to access the information;

20 generating a seed value;

21 producing a first hash seed value based on the seed value using a one-way  
22 hash function;

23 producing a second hash seed value based on the seed value and a user  
24 identifier using a keyed hash function;

25 generating a user storage key from the second hash seed value;

1 encrypting the information using the user storage key; and  
2 associating the access predicate with the encrypted information.

3  
4 5. (Canceled)

5  
6 6. (Previously presented) A computerized method for key-based  
7 secure storage comprising:

8 downloading information and an access predicate that specifies  
9 requirements for an application to access the information;

10 obtaining a storage key;

11 encrypting the information using the storage key;

12 associating the access predicate with the encrypted information;

13 obtaining an operating system storage key;

14 encrypting the access predicate with the operating system storage key; and

15 encrypting a plurality of other storage keys using the operating system  
16 storage key, wherein the other storage keys are selected from the group consisting  
17 of application storage keys and user storage keys.

18  
19 7. (Previously presented) A computerized method for key-based  
20 secure storage comprising:

21 downloading information and an access predicate that specifies  
22 requirements for an application to access the information;

23 obtaining a storage key;

24 encrypting the information using the storage key;

25 associating the access predicate with the encrypted information;

1 generating a seed value;

2 generating an operating system storage key based on the seed value; and

3 encrypting the access predicate with the operating system storage key.

4  
5 8. (Previously presented) A computerized method for key-based  
6 secure storage comprising:

7 downloading information and an access predicate that specifies  
8 requirements for an application to access the information;

9 generating a seed value for the application;

10 producing an application hash seed value based on the seed value for the  
11 application using an application-specific one-way hash function;

12 generating an application storage key from the application hash seed value;

13 generating a seed value for a user;

14 producing a first user hash seed value based on the seed value for the user  
15 using a one-way hash function;

16 producing a second user hash seed value based on the first user hash seed  
17 value and a user identifier using a keyed hash function;

18 generating a user storage key from the second user hash seed value, the  
19 application storage key and the user storage key to encrypt information containing  
20 a portion specific to an application and a portion specific to the user;

21 encrypting the information using the application storage key and the user  
22 storage key; and

23 associating the access predicate with the encrypted information.  
24  
25

1           9.     (Previously presented)     A computerized method for key-based  
2 secure storage comprising:

3           downloading information and an access predicate that specifies  
4 requirements for an application to access the information;

5           obtaining a storage key;

6           encrypting the information using the storage key;

7           associating the access predicate with the encrypted information;

8           storing the storage key in a key vault provided by a third-party; and

9           recovering the storage key from the key vault.

10  
11          10.    (Original)    The computerized method of claim 9, wherein  
12 recovering the storage key comprises:

13          requesting recovery of the storage key; and

14          providing information to the third-party to enable validation of the request.

15  
16          11.    (Previously presented)    The computerized method of claim 9,  
17 further comprising:

18          selecting the key vault from a plurality of key vaults provided by a trusted  
19 operating system.

20  
21          12.    (Previously presented)    The computerized method of claim 9,  
22 further comprising:

23          selecting the key vault designated by a provider of the information.

24  
25          13-14. (Canceled)

1  
2 15. (Previously presented) A computer system comprising:  
3 a processing unit;  
4 a system memory coupled to the processing unit through a system bus;  
5 a computer-readable medium coupled to the processing unit through a  
6 system bus;  
7 a generate key function executed from the computer-readable medium by  
8 the processing unit, wherein the generate key function causes the processing unit  
9 to generate an operating system storage key based on an identity for the operating  
10 system and based on a seed.

11  
12 16. (Previously presented) A computer system comprising:  
13 a processing unit;  
14 a system memory coupled to the processing unit through a system bus;  
15 a computer-readable medium coupled to the processing unit through a  
16 system bus;  
17 a generate key function executed from the computer-readable medium by  
18 the processing unit, wherein the generate key function causes the processing unit  
19 to generate an operating system storage key based on an identity for the operating  
20 system;  
21 an application specific one-way hash function executed from the  
22 computer-readable medium by the processing unit, wherein the application  
23 specific one-way hash function causes the processing unit to generate an  
24 application storage key from a hashed seed; and  
25

1 a generate application key function executed from the computer-readable  
2 medium by the processing unit, wherein the generate application key function  
3 causes the processing unit to generate the hashed seed from an application seed.

4  
5 17. (Previously presented) A computer system comprising:  
6 a processing unit;  
7 a system memory coupled to the processing unit through a system bus;  
8 a computer-readable medium coupled to the processing unit through a  
9 system bus;

10 a generate key function executed from the computer-readable medium by  
11 the processing unit, wherein the generate key function causes the processing unit  
12 to generate an operating system storage key based on an identity for the operating  
13 system;

14 a key-hash function executed from the computer-readable medium by the  
15 processing unit, wherein the key-hash function causes the processing unit to  
16 generate a user storage key from a hashed seed and an identity for the user;

17 a one-way hash function executed from the computer-readable medium by  
18 the processing unit, wherein the one-way hash function causes the processing unit  
19 to generate the hashed seed from a previously hashed seed; and

20 a generate user key function executed from the computer-readable medium  
21 by the processing unit, wherein the generate user key function causes the  
22 processing unit to generate the previously hashed seed from a user seed.

23  
24 18. (Canceled)  
25

1           19.   (Currently amended)       A computer system comprising:  
2           a processing unit;  
3           a system memory coupled to the processing unit through a system bus;  
4           a computer-readable medium coupled to the processing unit through a  
5           system bus; and  
6           a trusted operating system executed from the computer-readable medium by  
7           the processing unit, wherein the trusted operating system causes the processing  
8           unit to:  
9                 encrypt downloaded information using a storage key based on a seed  
10                value,  
11                ~~to~~ encrypt an access predicate associated with the downloaded  
12                information using an operating system storage key,  
13                ~~to~~ encrypt the seed value for the storage key using the operating  
14                system storage key, and  
15                ~~to~~ associate the encrypted access predicate with the encrypted seed  
16                value.

17  
18           20.   (Previously presented)   The computer system of claim 19,  
19           wherein the trusted operating system further causes the processing unit to validate  
20           each application requesting access to the downloaded information using the access  
21           predicate, and decrypts the seed value for use by a validated application.

22  
23           21.   (Previously presented)   The computer system of claim 19,  
24           wherein the storage key used to encrypt the downloaded information is specific to  
25           an application.

1  
2 22. (Previously presented) A computer system comprising:  
3 a processing unit;  
4 a system memory coupled to the processing unit through a system bus;  
5 a computer-readable medium coupled to the processing unit through a  
6 system bus; and  
7 a trusted operating system executed from the computer-readable medium by  
8 the processing unit, wherein the trusted operating system causes the processing  
9 unit to encrypt downloaded information using a storage key based on a seed value,  
10 and wherein the storage key used to encrypt the downloaded information is  
11 specific to a user.

12  
13 23-24. (Canceled)

14  
15 25. (Previously presented) A computerized method for key-based  
16 secure storage comprising:  
17 downloading information and an access predicate that specifies  
18 requirements for an application to access the information;  
19 obtaining a storage key;  
20 encrypting the information using the storage key;  
21 associating the access predicate with the encrypted information;  
22 storing the storage key in a key vault provided by a third-party;  
23 recovering the storage key from the key vault; and  
24 selecting the key vault from a plurality of key vaults provided by an  
25 authenticated operating system.



1  
2 26. (Canceled)

3  
4 27. (Previously presented) A computer system comprising:  
5 a processing unit;  
6 a system memory coupled to the processing unit through a system bus;  
7 a computer-readable medium coupled to the processing unit through a  
8 system bus; and  
9 an authenticated operating system configured to execute on the processing  
10 unit from the computer-readable medium, the authenticated operating system  
11 causing the processing unit to encrypt downloaded information using a storage key  
12 based on a seed value;  
13 wherein the authenticated operating system further causes the processing  
14 unit to encrypt an access predicate associated with the downloaded information  
15 using an operating system storage key, to encrypt the seed value for the storage  
16 key using the operating system storage key, and to associate the encrypted access  
17 predicate with the encrypted seed value.

18  
19 28. (Previously presented) The computer system of claim 27, wherein  
20 the authenticated operating system further causes the processing unit to validate  
21 each application requesting access to the downloaded information using the access  
22 predicate, and decrypts the seed value for use by a validated application.  
23  
24  
25

1           29.   (Previously presented) The computer system of claim 27, wherein  
2 the storage key used to encrypt the downloaded information is specific to an  
3 application.

4  
5           30.   (Previously presented) The computer system of claim 27, wherein  
6 the storage key used to encrypt the downloaded information is specific to a user.